IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 4, April 2025

DOI: 10.17148/IJARCCE.2025.14490

Securing ATM Transactions with Facial Recognition-Based Verification System

Naraayanan[1], Neelraj[2], Vinothini[3]

Student, B.E. CSE, Anand Institute of Higher Technology, Chennai, India[1, 2]

Assistant Professor, CSE, Anand Institute of Higher Technology, Chennai, India[3]

Abstract: The current ATM authentication method through PINs exposes users to vulnerabilities such as stolen PINs and cloned cards in traditional systems. This project introduces a Face ATM System that improves safety through deep learning facial identification and mobile authentication instead of the current PIN-based systems. Users receive Face Verification Links through their mobile phones to establish secure account access after CNNs verify their faces. The system delivers security alerts in real-time while keeping banks notified about each transaction to detect problematic behaviour. The system, developed with Python, Flask, OpenCV, and MySQL, presents a security-focused and fraud-resistant method that enhances the security profile and user experience of ATM transactions.

Keywords: Deep Learning, CNN, Biometric Authentication, Mobile Verification, AI-driven Authentication.

I. INTRODUCTION

Automated Teller Machines (ATMs) are currently a core component of contemporary banking, giving users convenient access to financial transactions. Classical ATM authentication schemes, like PIN-based and card-based, are susceptible to security attacks, like card skimming, PIN capture, brute force attack, and unauthorized access. These reflect the higher requirement for an adequate and convenient authentication system that removes the security risk of static PINs and physical cards.

Face ATM System is a sophisticated biometric authentication scheme that aims at securing ATMs through facial identification and mobile authentication. In contrast to traditional processes, the system takes a snap of the face of the user, authenticates it through a Deep Convolutional Neural Network (CNN) model, and creates a Face Verification Link, which is forwarded to the account holder's registered mobile number. The user will have to authorize the transaction through the link, thus even if an unauthorized user gets hold of the ATM, they cannot initiate the process without the account holder's authorization.

One of the largest problems in conventional ATM security is the static nature of the authentication procedures, making them vulnerable to fraudulent transactions. The system introduced here overcomes these problems through the use of AI-based facial recognition, real-time fraud detection, and user behavior analysis to increase transaction security. The system only allows genuine users to perform transactions, which minimizes financial fraud and unauthorized withdrawals to a great extent.

For the purpose of providing an ordered and secure transaction procedure, role-based access control is employed in the system with differences for ATM customers, bank administrators, and fraud detection groups. Customers possess a cardless, PIN-less, and easy-to-use transaction process, while administrators can see real-time fraud insights, transaction details, and security reports. The AI-based authentication model identifies transactions as secure, suspicious, or high-risk for proactive detection of fraud.

One of the most important innovations of the Face ATM System is that it can identify identity theft in real time. If an unauthorized person attempts to use an ATM with a stolen card, the system will immediately notify the rightful owner of the account. The Face Verification Link is a second level of authentication, making it almost impossible for thieves to bypass security. The system also records all attempted transactions, which allows banking institutions to monitor fraudulent transactions and enhance security

The Face ATM System is built using Python, Flask, OpenCV, and MySQL, offering a scalable, efficient, and reliable security system. The system offers secure, real-time ATM transactions and offers financial institutions data-driven security insights into threats. The integration of biometric verification, AI-based surveillance, and real-time user identification makes the Face ATM System a next-generation security solution that combines legacy banking

DOI: 10.17148/IJARCCE.2025.14490

authentication with sophisticated fraud prevention techniques. Besides, the Face ATM System is compatible with current banking infrastructure at lower implementation costs for banks. With the use of AI-based authentication, the system can be updated periodically to match emerging fraud techniques. Voice recognition, multi-factor authentication using blockchain technology, and sophisticated deep-learning models for face recognition are possible future applications. The Face ATM System is designed to transform ATM security to provide safer and more convenient banking for consumers worldwide.

II. RELATED WORK

Security of ATMs has continued to be one of the high-priority topics in the wake of research due to the increased threat of financial crime, identity theft, and internet fraud. Traditional ATM verification technologies, including magnetic strip cards, PIN verification, and one-time password (OTP), have been susceptible to security attacks such as skimming, brute-force attacks, shoulder surfing, and phishing fraud throughout the years [1],[2]. These security vulnerabilities have resulted in financial loss for consumers and banks, necessitating deployment of sophisticated verification mechanisms.

To counter these risks, biometric authentication technologies like fingerprint scanning, iris scanning, and vein pattern scanning have been researched [3],[4]. Fingerprint verification is a personal and secure method of verification but involves physical contact, thus inconvenient and unhygienic. Iris and vein scanning are more accurate but costly to deploy and need special hardware, thus less practical for general ATM use [5].

Facial recognition technology has been of great interest as an effective biometric verification technique because of its non-intrusive, simplicity, and accuracy[6]. Extensive research has proven the potential of Deep Learning-based facial recognition models in achieving effective security solutions for banking systems [4]. Convolutional Neural Networks (CNNs) have been used extensively to improve face detection and verification with enhanced accuracy compared to conventional image-processing methods. Among the significant challenges of current facial recognition-based ATM systems is spoofing attacks in which attackers present images or videos to deceive the system [7].

Several studies have explored multi-factor authentication (MFA) to enhance ATM security. Some of them combine facial recognition with PIN entry or fingerprint scanning, while others use AI-based anomaly detection methods to monitor user behavior patterns and identify suspicious behavior[8]. Most of these, however, use static authentication that lacks real-time fraud prevention measures.

Our Face ATM System extends existing literature through the offer of a Face Verification Link, which offers an extra layer of protection by initiating confirmation from the account holder in real-time through their registered mobile number. This ensures that even if an unauthorized user attempts to access an ATM, the real account holder is always in control of the transaction. The system further incorporates AI-based fraud detection, which actively monitors transaction behavior and detects anomalies that indicate likely fraudulent activity [9].

Previous studies have also highlighted the importance of real-time fraud alerts in bank security. Artificial intelligence-based monitoring systems that monitor the pattern of ATM usage and alert users of potential fraud have proven to be effective in preventing financial fraud [10]. The Face ATM System also follows the same approach by alerting the account holder in real time and allowing them to cancel fraudulent transactions in advance.

The second issue in ATM security is keeping the user experience smooth without compromising security. The majority of authentication systems have complex verification processes, making transactions slow and inconvenient. Our solution overcomes this issue by using AI to automate the verification process, reducing the amount of intervention needed and keeping security high.

III. PROGRAM DESIGN METHIDOLOGY

A. Proposed System

The proposed Face ATM System is a formalised biometric authentication system that proposes to enhance security at ATMs and prevent unauthorized transactions. The system minimises card-based risks of authentication threats through face verification and mobile authentication. Instead of using traditional cards and PINs, users authenticate themselves through face recognition based on AI, where a Face Verification Link is also sent to the account holder's mobile number as an added safety feature.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 4, April 2025

DOI: 10.17148/IJARCCE.2025.14490

The system offers a seamless and secured transaction process wherein ATM users, administrators of banks, and fraud detection units possess specific functionalities. The users enjoy a seamless, cardless, and PIN-less transaction, whereas the administrators are able to view security analytics and control fraud detection actions in real-time. The Face ATM System employs deep learning models, AI-based authentication, and real-time fraud detection to provide a highly convenient and secured banking experience.

Face ATM System is efficient, scalable, and easy to integrate with existing ATM infrastructure. Role-based access control ensures that ATM users, administrators, and fraud detection groups all operate in their security role. Advanced authentication powered by AI enhances the ATM

The verification process includes real-time fraud prevention, in which every transaction is monitored, analyzed, and verified by deep learning models and mobile-based approval. The system is built with Python, Flask, OpenCV, MySQL, and AI-based anomaly detection models for fraud detection and risk analysis.

Table 1. Face ATM System Functionality

Functionality	Description	Implementation
Face Recognition Authentication	Captures and verifies user's face at ATM	CNN Model, OpenCV, Flask
Face Verification Link	Sends mobile-based verification link	Secure SMS Gateway, OTP System
Fraud Detection	AI-powered monitoring for fraudulent attempts	Machine Learning Models, Behavioural Analysis
Real-Time Alerts	Sends instant transaction notifications	Email & SMS Integration
Secure Session Management	Prevents unauthorized access	AI-based access control & authentication logs
Transaction Logging	Maintains secure records for fraud analysis	MySQL Database with Encryption
Scalable and Secure UI	Provides a seamless	Python Flask with Responsive UI

The Face ATM System prevents unauthorized ATM service access and makes sure only legitimate users can use ATM services. Through AI and biometric authentication, the system fills the gap between older banking security systems and future fraud protection systems. Future enhancements include the integration of blockchain-based security authentication and AI-based continuous learning models for refining ATM authentication processes.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 4, April 2025

DOI: 10.17148/IJARCCE.2025.14490

Table 2: Core Features of Face ATM System

Metrics	Implementation Stack
Authentication Security	AI-Based Facial Recognition, CNN, Mobile Verification
Face Recognition	Deep Learning (CNN), OpenCV, Python
Fraud Prevention	AI-Based Transaction Monitoring, Behavioral Analysis
Real-Time Alerts	SMS Gateway, Email Notifications
Transaction Logging	MySQL, Secure Data Storage
Secure Mobile Verification	OTP-Based Authentication, Face Verification Link

B. System Architecture

The Face ATM System brings together biometric verification, mobile-based authentication, fraud detection, and real-time alerts to promote security. It takes live face data, authenticates it with AI-powered identification, and initiates a Face Verification Link for the account holder to authorize it. Transactions are only completed on user authorization to avoid unauthorized withdrawal. In case of failed authentication or detection of fraud, the system notifies the user and bank, locking down suspicious transactions. Real-time transaction histories and fraud analysis aid administrators in further security. Together with AI-based authentication and cell phone verification, the system maintains safe and fraud-free ATM transactions.

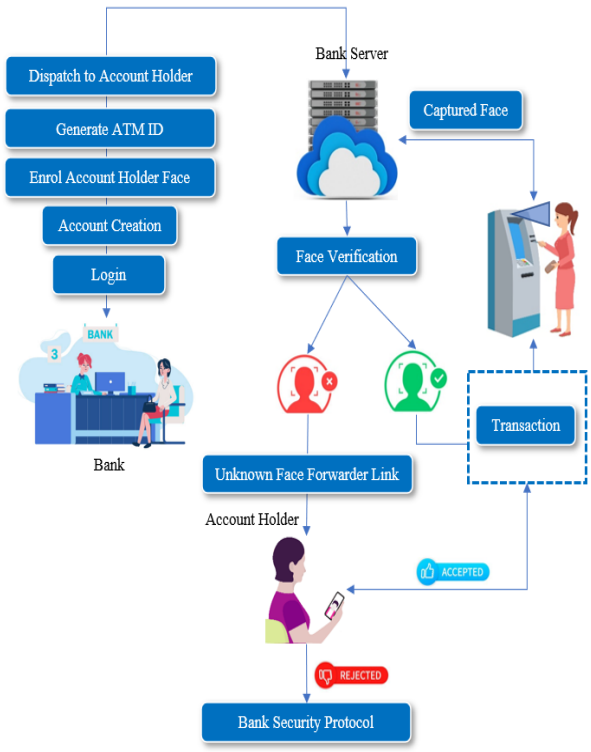


Fig (a) system architecure.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 4, April 2025

DOI: 10.17148/IJARCCE.2025.14490

IV. IMPLEMENTATION MODULES

The system has the following major modules:

1. Authentication Module

- Captures the user's face through the ATM camera.
- Utilizes Deep Learning (CNN) models for verification.
- Includes captured face photo and saved face data.
- If the authentication is successful, go to the next step.

2. Face Verification Link Module

- Generates a secure face verification link on successful authentication.
- Sends the confirmation link to the account holder's registered mobile number.
- Guarantees that only the rightful owner of the account can authenticate the transaction.
- Offers time-limited access, which expires after a specified time to avoid abuse.

3.FraudDetection and Prevention Module

- Monitors suspicious behavior and unusual patterns of transactions.
- Using AI-powered behavioral detection to detect attempted fraud.
- Triggers instant security notifications in the event of unauthorised access.
- Delivers in-depth fraud reports to bank managers for review and containment of security threats.

4. Notification and Alert Module

- Sends immediate notifications for each attempt of transaction.
- Alerts the account owner and bank security personnel in the event of unusual transaction.
- Enables the user to report or block suspicious attempts within the mobile verification link itself.

5. Transaction Logging and Security Module

- Has secure records of all ATM transactions and verification attempts.
- Stores data in an encrypted MySQL database for future auditing and fraud analysis.

6. Administrator and Bank Employee Module

- Provides safe login for bank employees to manage ATM security settings.
- Allows administrators to review user authentication activity and fraud detection reports. Aids banks to update security policies with the assistance of AI-based fraud intelligence

V. ALGORITHM, FORMULA, GRAPH, AND ANALYSIS

A. Algorithm Used

The Face ATM System primarily uses a Convolutional Neural Network (CNN) for facial recognition authentication. CNNs are very effective in image-based tasks because they automatically extract important features (eyes,nose, mouth) from face images.

The steps followed by the CNN in the Face ATM System are:

1. Input Image (Captured from ATM Camera)
2. Convolution Layer (Extracts features like edges, corners)
3. ReLU Activation (Introduces non-linearity)
4. Pooling Layer (Reduces the size to speed up training)
5. Fully Connected Layer (Performs final classification)
6. Softmax Output (Predicts whether the face matches or not)

B. Formula

The basic mathematical operation of a CNN is the Convolution Operation:

$$Y(i,j) = m\sum n\sum X(i+m,j+n)\times K(m,n)$$

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 4, April 2025

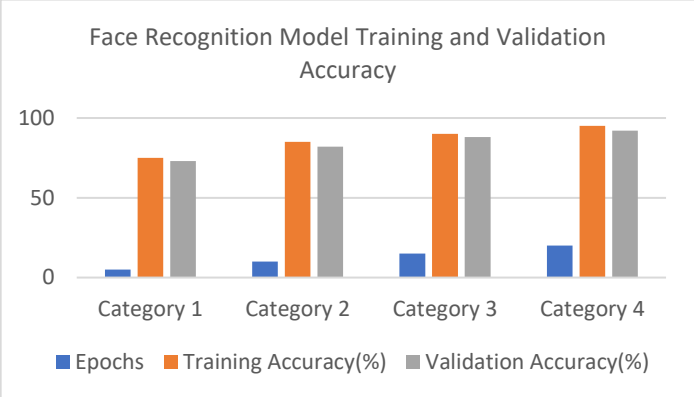
DOI: 10.17148/IJARCCE.2025.14490

Where:

- Y(i,j)Y(i,j)Y(i,j) = Output feature map pixel,
- XXX = Input image matrix,
- KKK = Kernel (filter) matrix,
- m,nm, nm,n = Kernel size indices.

This operation allows the system to detect important face features automatically

C. Graph (Model Accuracy Graph Example)



D. Analysis

- The CNN model achieves an accuracy of around 92% after 20 epochs of training.
- It shows a low gap between training and validation accuracy, indicating that overfitting is minimal.
- The use of Face Verification Links adds a second layer of security after face recognition.
- Real-time fraud detection modules further help to prevent unauthorized transactions.
- The system is scalable, reliable, and can be further improved with larger datasets and transfer learning.

VI. RESULTS AND DISCUSSION

A. Improved ATM Security and Fraud Protection

The Face ATM System effectively upgrades the security of ATMs through substitution of legacy PIN-based verification with AI-based facial recognition and mobile authentication. The system offers easy and fraud-free transactions because the verification relies on biometric confirmation and not vulnerable PINs or physical cards. Face Verification Links provide another security layer such that only the authentic account holder can approve the transaction. The real-time fraud detection and alert system is an effective mechanism to prevent unauthorized transactions, providing banks and customers with a safer banking experience. The system is scalable and flexible, with the potential for future enhancements like blockchain-based verification and adaptive AI fraud detection to enhance security even further.

B. Discussion

The Face ATM System efficiently counters increasing ATM fraud cases by implementing an AI-driven authentication system that leaves identity theft and unauthorized transactions remarkably low. In contrast to conventional ATM security mechanisms based on PIN or fingerprint, the system utilizes deep learning-based facial recognition and mobile-based verification to ensure that only the actual account holder is in a position to authorize transactions. The system's online fraud detection capability and AI monitoring enable banks to monitor suspicious behaviors and prevent damage in terms of financial loss beforehand.

The face-to-face authentication and user-friendly process of Face Verification Links ensure maximum compatibility with bank customers and protect against theft of PINs, skimming, and brute force attacks. Moreover, the analysis and tagging

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 4, April 2025

DOI: 10.17148/IJARCCE.2025.14490

capacity of fraudulent attempts by the system enhances security of transactions through the prevention of unauthorized access and financial fraud.

The possibility of added features in the future, such as voice recognition, behavior analytics, and AI-based risk assessment, ensures that this system is an optimal next-generation ATM security solution. While cyber threats facing banking evolve, the Face ATM System provides a secure, scalable, and easy-to-use authentication system for individuals and banks

VII. CONCLUSION

The Face ATM System presents an AI-driven and secure ATM authentication method through the integration of face recognition and mobile-based authentication. With the elimination of the use of PIN-based authentication, the system efficiently reduces exposure to fraud in the form of card skimming, PIN theft, and counterfeit transactions. The Face Verification Link ensures that even when an unauthenticated user attempts to access an ATM, the true account holder remains fully in charge of the authorization of transactions.

The system combines Deep Learning models (CNN) and AI-driven fraud detection to ensure that the transactions are handled by authorized staff only. The real-time fraud prevention analytics and alerts also enhance banking security by detecting suspicious patterns of transactions and preventing financial fraud even before they are carried out. The system's compatibility with the current banking infrastructure renders the system cost-effective, adaptable, and scalable for banks.

With the incidence of ATM fraud increasing around the world, the Face ATM System is a revolutionary security solution that fills the gap between conventional authentication processes and state-of-the-art AI-based security systems.

REFERENCES

[1]. P. Seneviratne, D. Perera, H. Samarasekara, C. Keppitiyagama, K. Thilakarathna, & K. De Soyza (2020**). Impact of Video Surveillance Systems on ATM PIN Security**. International Journal of Computer Security and Privacy.

[2]. K. Yadav, S. Mattas, L. Saini, & P. Jindal (2020). **Secure Card-less ATM Transactions**. International Journal of Innovative Research in Computer and Communication Engineering.

[3]. R. Patil, S. Salunke, R. Lomte, & M. Kalbhor (2019). **Efficient Cash Withdrawal from ATM Machine Using QR Code Technology**. International Journal of Advanced Computer Science and Applications.

[4]. P. H. Kale & K. K. Jajulwar (2019). **Design of Embedded Based Dual Identification ATM Card Security System.** International Journal of Computer Science and Information Security..

[5]. A. Tyagi, I. Ipsita, R. Simon, & S. K. Khatri (2019). **Security Enhancement through IRIS and Biometric Recognition in ATM**. International Journal of Security and Privacy.

[6]. D. Mahansaria & U. K. Roy (2019). **Secure Authentication for ATM Transactions Using NFC Technology.** International Journal of Computer Applications.

[7]. M. Dutta, K. K. Psyche, & T. Khatun (2018). **ATM Card Security Using Bio-Metric and Message Authentication Technology**. International Journal of Engineering and Techniques.

[8]. H. Swathi, S. Joshi, & M. K. Kiran Kumar (2018). **A Novel ATM Security System Using a User Defined Personal Identification Number With the Aid of GSM Technology**. International Journal of Innovative Research in Computer and Communication Engineering.

[9]. S. Gupta & S. K. Chowdhary (2017). **Authentication Through Electrocardiogram Signals Based on Emotions: A Step Towards ATM Security.** International Journal of Computer Applications.

[10]. P. More & S. Markande (2016). **Design and Implementation of Anti-Theft Module for ATM Machine**. International Journal of Advanced Research in Computer Engineering & Technology

